Universitatea Politehnică Bucureşti

Facultatea de Electronică, Telecomunicaţii şi Tehnologia Informaţiei

**Reţele de calculatoare**

“NAT - Translatarea adresei de rețea”

**Studenţi:**Iordache Florin-Dorian

Iordache Cătălin-Ionuţ

**Grupa:** 442A (CTI)

Anul universitar

2014-2015

**CUPRINS:**

**Capitolul 1**(Iordache Florin-Dorian)

Introducere generală – Prezentare tema................................................pag.3

**Capitolul 2**(Iordache Florin-Dorian)

   2.1 Tipuri de NAT.............................................................................pag.3

2.1.1 Translatare statica.................................................pag.3  
            2.1.2 Translatare dinamica.............................................pag.3  
            2.1.3 Translatarea adreselor cu supraincarcare (PAT).......pag.4 2.2 Principii de implementare si functionare............................... pag.5

**Capitolul 3**(Iordache Florin-Dorian)

Necesitatea utilizarii maparii pe o singura adresa publică........................pag.8

**Capitolul 4**(Iordache Cătălin-Ionuţ)  
  4.1 Dezavantaj al dispozitivelor NAT: Intarzirea disponibilitatii IPv6.................pag.9  
4.2 Avantajele protocolului NAT ...................................................................pag.10

4.3 Intîrzirea disponibilităţii IPv6 ...........................................................pag.11

4.4 Solutie: Mecanismul de transmitere in tunel. Tehnologia de tranzitie

TEREDO......................................................................pag.11

**Concluzii**(Iordache Cătălin-Ionuţ).........................................................pag.14

**Bibliografie**

**1.Introducere**

NAT(Network Address Translation-translatarea adresei de rețea) este procesul prin care adresa IP sursă sau adresa IP destinație este transformată într-o alta, prin modificarea antetului pachetelor IP.

NAT se refera la modul in care produce comunicatia intre nivelele retea ale utilizatorilor sau masini ce doresc sa schimbe informatie.

In prezent NAT este foarte des folosita in mapare mai multor adrese private pe o singura adresa publica. Această utilizare este cunoscută ca PAT (Port Address Translation) sau NAPT (Network Address Port Translation).

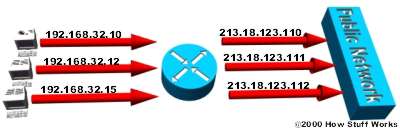
Pentru identificarea dispozitivelor conectate in retea se foloseste adresa IP.

**2.1 Tipuri de NAT**

**2.1.1 Translatare statică**

În cazul translatării statice, ruterul poate de fiecare dată sa asigneze o adresă IP externă unei cereri ,iar pachetele care pleacă de la un calculator,pleacă mereu cu aceeași adresă.

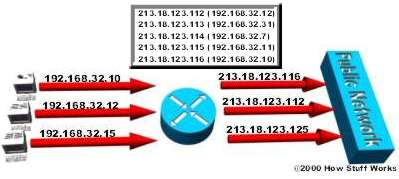
Translatarea statică a adreselor necesită construierea unei tabele de translatare ce va mapa mereu aceeași adresă privată pentru o adresă publică. În acest caz trebuie să existe număr egal de adrese publice și private, ceea ce nu e avantajos.Modul de funcționare a protocolului NAT static este ilustrat în figura de mai jos.



NAT static

**2.1.2 Translatare dinamica**

Translatarea dinamica a adreselor necesita existenta unui interval de adrese publice (address pool) urmand ca acestea sa fie mapate ulterior adreselor private din reteaua locala, in functie de ordinea in care statiile solicita comunicarea cu exteriorul. Daca coexiunea unei statii cu exteriorul s-a terminat, atunci adresa publica este returnata in intervalul de adrese disponibile (address pool), putand fi refolosita pentru maparea altei statii. Astfel, avem nevoie de un numar redus de adrese publice, comparativ cu translatarea statica.In figura de mai jos se poate vedea modul de lucru al protocolului NAT dinamic.



NAT dinamic

**2.1.3 Translatarea adreselor cu supraîncărcare (PAT)**

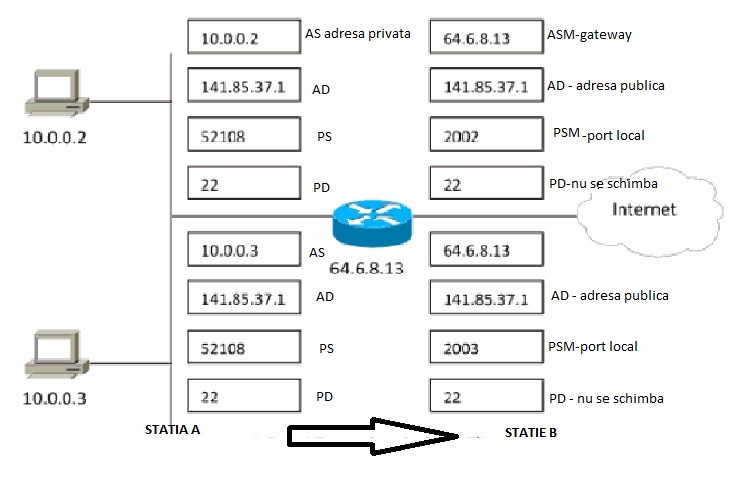
Este cea mai raspandită formă de NAT. Este cunoscută și sub denumirea de NAT multi-la-unu sau PAT( port address translation). PAT împrumută principiile NAT-ului de bază(translatarea dinamică – translatare adreselor IP) și în plus extinde conceptul de translatare și la nivelul porturilor.

PAT=translatare de IP + translatare de porturi.

Se considera urmatorul exemplu: Avand 250 de statii in reteaua locala care impart 20 de adrese publice. Daca 20 de statii schimba in acelasi timp informatii in exterior, ce se va intampla atunci cand a 21-una statie va incearca sa trimita in exterior pachete? Nu va putea trimite si primi nimic pentru ca nu mai sunt adrese publice de translatat, ele fiind deja mapate.

Solutia in aceste caz este translatarea porturilor pentru a multiplexa adresele private. Plecam de la ipoteza: combinatia intre adresa si port defineste UNIC o conexiune! In momentul in cand trecem dintr-o retea privata in una publica, putem modifica atat adresa IP cat si numarul portului din headerul tcp sau udp. Acesta metoda implica folosirea unui router capabil sa faca maparea adreselor si a porturilor. Dezavantajul este ca implica o complexitate marita si posibile probleme de compatibilitate.

Pentru o comunicaţie intre Statia A catre statia B,headerul pachetului din reţeaua privată cu adresa sursa AS, adresa destinaţie AD, portul sursă PS, portul destinaţie PD va fi înlocuit cu un nou header: adresa sursă: ASM(adresa routerului), adresa destinaţie nemodificată AD, port sursă PSM (port local). Portul destinaţie nu se schimbă, ramăne PD. Se memorează asocierea (AS,PS) – PSM.



Exemplu de PAT

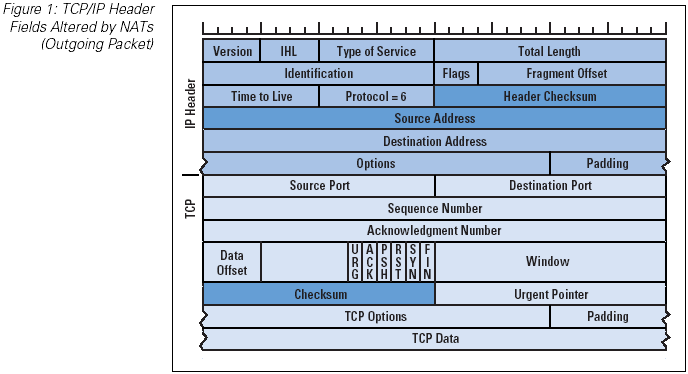
Dacă se transmite de la stația B la stația A(din exterior in interior), pachete ingoing (adresa sursă AD, adresa destinație ASM, portul destinație PSM ) atunci pachetul de inlocuiește cu unul având adresa destinație AS, adresa sursă ASM, portul destinație PS si va fi trimis in rețeaua locală. Portul sursă nu se modifică.

**2.2 Principii de implementare şi funcţionare – NAT de bază**

Principiu: Am un numar mic de staţii/hosturi dintr-o reţea privată ce necesită să comunice cu exteriorul reţelei. Dacă fiecărei staţii i se alocă o adresă IP dintr-o listă oficială de adrese disponibile/interval de adrese(address pool) numai atunci când staţia solicită accesul în exterior, atunci este necesar numai un număr relativ mic de adrese oficiale.

NAT este un translator de IP header, şi în particular NAT este un translator de adrese ip. Headerul unui pachet IP conţine sursa şi destinaţia adresei ip. Se admit 2 ipoteze:

* Dacă pachetul este transmis din interiorul reţelei locale către exterior(“outgoing”), în internet, atunci nat pe de o parte rescrie adresa sursă în headerul packetului cu altă valoare, şi pe de altă parte, alterează suma de control din header pentru a marca schimbarea facută in campul de adresă.
* Dacă un pachet este primit din exterior, destinat unei staţii din interiorul reţelei (“ingoing”), atunci adresa de destinaţie este rescrisă cu altă valoare, şi se recalculează iar suma de control.



Câmpuri alterate de NAT din headerul TCP/IP (pachet “outgoing”)

OBSERVAŢIE: Reţeaua locală, “interiorul” foloseşte adrese din cele private, ceea ce defineşte unicitatea doar la nivelul reţelei locale, nu şi in exterior.

Ce se întâmplă fără NAT?

În exemplu de mai jos se observă faptul că pachetul outgoing va fi transmis cu success pentru că are o adresă destinaţie publică 192.9.200.1 şi routerul va ştii în ce reţea să îl routeze, pe când pachetul ingoing nu va ajunge la destinaţie pentru că are o adresă destinaţie privată: 10.0.0.1, care nu este unică în internetul public. Hostul A foloseşte prima dată DNS(domanin name system) pentru a găsii adresa ip publică pentru hostul B, şi pe urmă trimite pachet având la adresa de destinaţie, adresa hostului B şi ca adresă sursă adresa locală a hostului A. Dacă pachetul a fost primit de hostul B fără alte alterări, staţia B nu ar mai fi în stare să răspundă.

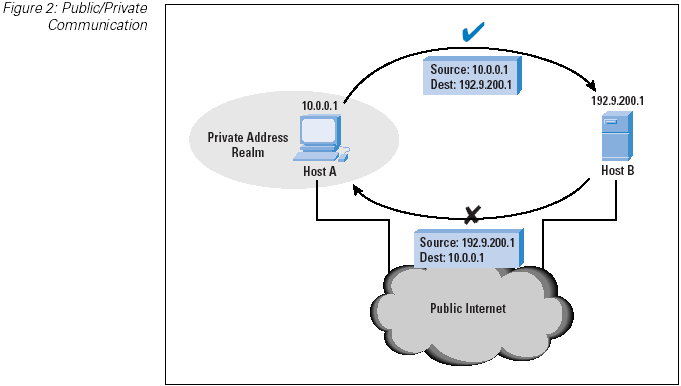


Figura 2: Comunicatia publica/privata

Ce se întâmplă cu NAT?

Studiem cele două ipoteze:

[Host A trimite către host B] Dacă am plasa un translator NAT între cele două hosturi, acesta ar intercepta pachetul de la hostul A la hostul B şi ar rescrie adresa sursă cu o adresă publică. NAT este configurat cu un interval de adrese publice, iar când o staţie din reţeaua locală trimite un pachet în exterior, se alege o adresă din acest interval care se mapează ca o adresă alias temporară adresei locale a staţiei A[alias: 139.130.1.1]. Aceast alias este folosită ca noua adresă sursă pentru pachet. La fel se va întampla şi cu celelate pachete.

[Host B trimite către host A] Dacă un pachet ar ajunge în reţeaua locală din exterior, prima oară se verifică adresa destinaţie. Dacă este una din intevalul de adrese ale NAT-ului, NAT-ul va căuta în tabela de translaţie adresa corespunzătoare mapării pe adresa publică respectivă, şi adresa de destinaţie este mapată adresei locale interne. Se recalculează suma de control şi se trimite pachetul mai departe. Dacă în schimb, adresa nu se află în intervalul de adrese al NAT-ului, se face drop la pachet.

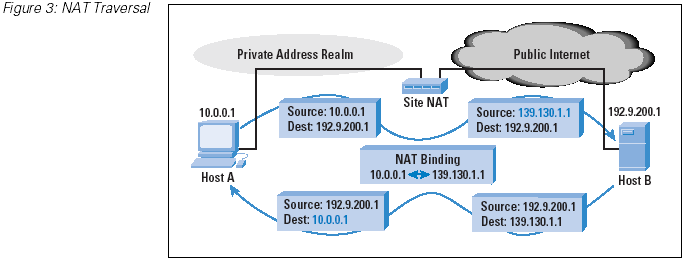


Figura 3 – Traversarea pachetelor cu NAT[4]

Serviciul NAT urmăreşte continuu asocierile făcute între adresele IP interne şi adresele IP externe.

Această mapare este valabilă un anumit timp. NAT-ul dispune de un timer care contorizează timpul care trece de la ultimul pachet ce trece cu acea adresă mapată. Dacă se depăşeşte o anumită valoare, atunci asocierea între cele 2 adrese dispare.

**3.Necesitatea utilizării mapării pe o singură adresă publică**

Conservarea spaţiului de adresă a devenit o problemă importantă a utilizării internetului, ca dovadă upgrade-ul de la varsiunea 4 a protocolului IP (ipv4) la versiunea 6 a protocolului IP (IPv6), proiectat iniţial să asigure un spaţiu de adrese mult mai mare, cât şi servicii suplimentare în scopul prelucrării rapide a pachetelor.

O procedură utilizată pentru a conserva spaţiul de adresare este de a modifica regula care impune ca adresele IP să fie unice la nivel global. Astfel, o parte din spaţiul de adresă global este rezervat pentru reţelele care nu sunt conectate la internet.

Scopul pe care il propune protocolul NAT este de a defini un mecanism ce permite adreselor IP să fie partajate de mai multe staţii.

Distingem 3 mulţimi de adrese pentru îndeplinirea acestui scop, adrese care nu sunt unice la nivel global, denumite în literatura de specialitate ca adrese private!

• O singura reţea de clasă A: 10.0.0.0/8 (10.0.0.0-10.255.255.255)

• Reţele consecutive de clasă B: 172.16.0.0/12 (de la 172.16.0.0 la 172.31.255.255)

• Reţele consecutive de clasă C: 192.168.0.0/16 de la 192.168.0.0 la 192.168.255.255

Routerele din cadrul unei reţele private, ce utilizează adrese private, vor limita referinţele la adresele private numai la nivelul unor legături interne. Aceste adrese private nu se pot ruta in INTERNET!

NAT este un exemplu de translatare a adreselor în reţea, (Network Address Tranlation). Accesul la Internet va fi indirect, se va face prin „intermediul unor pasarele de nivel aplicaţii(application gateways)” si nu cum ştim de obicei, direct prin intermediul nivelului IP cu ajutorul unei adrese IP private, care să localizeze în Internet fiecare utilizator.

Folosirea adreselor private oferă câteva avantaje:

• Schema de adresare rapidă şi comodă

• Metoda de securitate, pentru care adresele staţiior nu sunt accesibile în afara reţelei

Dar şi dezavantaje:

• Problema ridicată de acest principiu este capacitatea routerului de legatură între reţeaua privată şi exterior de a fi capabil să facă conversia adreselor private in adrese publice, deci să ruteze un serviu de NAT.

• Latenţa suplimententară pentru fircare pachet ce trece prin router.

• Limitarea plasării in interioul reţelei private a staţiilor ce oferă servicii publice, îngreunând conexiunile din exterior.

**4.1 Dezavantajele protocolului NAT**

Nu toate protocoalele pot să treacă de NAT. Exemple de astfel de protocoale ar fi H.323, SMTP.

Dacă NAT este folosit pentru conectarea mai multor utilizatori la acelaşi server se poate crea iluzia unui atac DoS (de exemplu mulţimea de utilizatori ICQ peste NAT poate aduce la probleme de conexiune cu serverul a unor utilizatori; o soluţionare parţială a problemei date ar fi folosirea unei grupe de adrese).

Limitarea numărului de staţii de lucru (maşini) la o adresă IP reală (rutabilă), ceea ce se explică prin limitarea numărului deporturi: 65536 – 4096 = 61440 de porturi disponibile.

Din protocoalele de nivelul 4 după modelul OSI NAT poate lucra doar cu TCP şi UDP, alte protocoale de transport nu pot fi folosite.

Protocolul NAT încalcă definirea modelului OSI, lucrînd simultan la 2 nivele (adresă IP – nivelul 3, numărul portului – nivelul 4) şi definirea dresei IP, care identifică o singură staţie de lucru.

Protocolul NAT, datorită translatării impune o întîrziere în timp a transmisiunii.

Diapazonul de adrese IP private este următorul:

10.0.0.0 – 10.255.255.255

172.16.0.0 – 172.31.255.255

192.168.0.0 – 192.168.255.255

**4.2 Avantajele protocolului NAT**

Permite economisirea adreselor IP, translatînd cîteva adrese IP interne într-o adresă IP externă rutabilă sau un număr de adrese IP interne mai mare într-un număr de adrese IP externe rutabile mai mic. După aşa un principiu sunt construite majoritatea reţelelor de comunicaţii din lume.

Permite preîntîmpinarea sau luimitarea adresării din exterior la hosturile din interior, totodată lăsînd posibilitatea adresării din interior în exteriorul reţelei. La iniţializarea conexiunii din interiorul reţelei se efectuează translatarea. Pachetele de răspuns, venite din exteriorul reţelei, corespuind translatării create şi pot trece. Însă dacă o astfel de translattare nua fost creată atunci pachetele nu pot trece.

Permite ascunderea anumitor servicii ale serverelor/hosturilor interne. În principiu, are loc aceiaşi translatare la un anumit port, însă există posibilitatea de a schimba un port a unui serviciu înregistrat pe un număr de port efemer (de exemplu portul 80 a serviciului http pe un port extern 54055). Astfel se ridică nivelul de securitate.

**4.3 Intîrzirea disponibilităţii IPv6**

Ipv6 este urmatoarea versiune a protocolului Ipv4, apărut din consideraţii de spaţiu de adresare şi servicii suplimentare(securitate, mobilitate). Cu timpul, din ce în ce mai multe dispozitive încep să folosescă Ipv6, şi apare problema indisponibilităţii translatării adreselor Ipv4, adică NAT. Pentru că ar fi costisitor ca toate dispozitivele NAT să fie actualizate sau înlocuite, cei de la Microsoft au implementat o metodă de transmitere în tunel, numite TEREDO. Deşi mai există mesanisme de tranziţie care tunelează ipv6 către ipv4 (exemple: ISATAP sau 6to4), acestea nu funcţioneaza şi la nivelul translatării de adrese, NAT.

Dacă o staţie care suportă Ipv6, se situează in spatele unui IpV4 NAT, apare o barieră în situaţia transmiterii/primirii pachetelor de la alte staţii Ipv6. O porţiune de reţea(care include NAT) între cele două capete ce suportă Ipv6 va fi indisponibilă la acest protocol.

**4.4 Soluţie: Mecanismul de transmitere in tunel. Tehnologia de tranziţie TEREDO**

Originar, protocolul s-a numit Shipworn. Teredo este o tehnologie de tranziţie intre Ipv6 si Ipv4 care facilitează conectivitatea IPv6 end-to-end între orice gazde IPv6/IPv4 amplasate în spatele unuia sau mai multor dispozitive NAT IPv4. Pachetele de date IPv6 sunt trimise ci ajutorul Tereodo intre utilizatori ca mesaje UDP bazate pe IPv4 .

Procesul de tunelare constă în încapsularea datelor unui protocol într-un alt protocol.

Teredo funcţionează tunelând protocolul Ipv6 pe un Port UDP Ipv4 cel puţin pe portiunea care acceptă numai Ipv4. Are un grad mare de automatizare. TEREDO stabileşte un tunel, de la client, prin NAT către un nod ce suportă ambele tehnologii. Astfel pachetele Ipv6 sunt tunelatare printr-un protocol UDP(folosind în cadrul NET, numărul portulului UDP). Fiecare pachet IPV6 e conţinut într-un header udp, care e transformat în interior într-un header IPV4.

Se definesc trei componente ale comunicaţiei cu ajutorul TEREDO:

• Clienţi – staţii care folosesc TEREDO ca să ajungă la alte staţii Ipv6 pentru a face schimb de date. (chiar dacă clienţii suportă mecanisme si Ipv4 si Ipv6 ei pot fi blocaţi în spatele unor dispozitive care suporta doar Ipv4 NAT). Clienţii teredo, trimit şi primesc mereu trafic teredo ipv6 tunelat în datagrame UDP peste Ipv4.



Figura – teredo încapsulează pachete ipv6 în UDP peste ipv4

• Relee teredo –routere ipv6 care primesc trafic destinat clienţilor teredo şi îl rutează mai departe serviciului teredo. Pachetele native ipv6 sunt încapsulate pentru transmisie în ipv4; când pachetele se primesc de la o reţea ipv4, sunt decapsulate în pachete ipv6.

• Servere teredo – ajută clienţii să stabilească tunele către staţii ipv6, determinând adresele lor teredo şi dacă NAT-ul respectiv este compatibil cu teredo. Nu poate fi considerat un releu general , chiar dacă se situează şi in Ipv4 şi in Ipv6. Prin ele trec doar mesaje despre protocol, nu permit routarea datelor/pachetelor.

Portul standard pe care serverele teredo le ascultă este portul udp 3544. Deocarece clientul se află în spatele unui ipv4 NAT, numărul portului extern pentru serviciul teredo nu este în general la fel cu portul local pe care se ascultă.

Pasi:

1. Procedura de calificare a clientului – se stabilesc adresa Teredo, se excută doar o dată, la activarea serviciului

2. Stabilirea căii

3. Trimiterea pachetului

Adresa Teredo

Este o adresa Ipv6(128 biti sau 16 octeti) ce conţine suficiente informaţii pentru un releu ca să acceseze clientul. 

- Formatul Adresei Teredo

Exemplu de adresa Teredo: 2001::4136:E37E:8000:EEFB:3FFF:DD59:

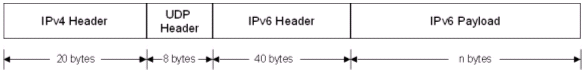
- Prefix 2001:0000::/32

- Server Ipv4 address, 32 biti, adresa teredo a serverului clientului, 4136:E37E rezultă adresa 65.54.227

- Câmpul de flaguri are 16 biti 8000

- Adresa mapata de NAT: 3FFF:DD59, adica 192.0.34.166

- Portul 4356 (0xEEFB) pentru serviciul teredo

Pachetele Teredo sunt transmise ca pachete UPD prin reţea IPV4. 

Aceste datagrame UDP sunt routate uşor în reţea ipv4 şi peste dispozitivele de conectare NAT. Faţă de alte protocoale de tranziţie ipv4-ipv6, Teredo are avantajul conectivităţii ipv4-ipv6 şi dincolo de routerele locale. (exemplu NAT).

Totuşi, această metodă este una temporară, idee de baza şi tendinţa fiind ca pe termen lung toate conexiunile să fie ipv6 nativ.

Limitările protocolului asociează o singură adresă ipv6 cu un singur tunel, deci nu este posibil să folosim un singur tunel teredo pentru a conecta hosturi multiple, spre deosebire de protocolul 6to4.

Releele teredo limitează lungimea de bandă disponibilă pentru clienţii teredo.

**CONCLUZII**

* NAT este cel mai util pentru maparea mai multor adrese private pe o singură adresă publică.
* Cea mai folosita forma in present este NAPT, sau PAT, translatarea de porturi, pentru mai buna gestionare a adreselor publice alias, şi pentru creşterea numărului de combinaţii de asocieri adrese private-adrese publice.
* De observat este că NAPT dizolvă puţin prinzipiile OSI, putând fi considerat un protocol ce lucrează pentru 2 niveluri OSI (adresa IP de la nivelul 3-reţea şi numărul portulului de la nivelul 4 - transport )
* O problemă majoră a acestui protocol este disponibilitatea Ipv6. Pentru aceasta cei de la Microsoft au implementat tehnica de tranziţie Teredo ce constă în încapsularea pachetelor ipv6 în datagrame udp iv46, putând fi astfel rutat in ipv4 prin dispozitivele NAT.

**BIBLIOGRAFIE**

Rețele de calculatoare – Editia a treia revizuita, Andrew S. Tanenbaum, Ed. Agora, an 1998

Rețele locale - Rughiniș R.,Rughiniș, R., Deaconescu, R., Ciorba, A., Doinea, B., Editura PRINTECH

Note curs, Arhitecturi de retele si internet, ARI, C. Vladeanu, an 2013

Anatomy: A Look Inside Network Address Translators – The Internet Protocol Journal, septembrie 2004, volumul7, nr 3, [www.cisco.com](http://www.cisco.com)

Învăţare automată trafic de traversare IPv6 NAT - <https://support.norton.com>

The teredo Protocol – Dr. James Hoagland, Ed.Symantec, anul 2007

<http://andrei.clubcisco.ro/cursuri/f/fsym/3rl/cursuri2012/RL_curs_09.pdf>

http://biblioteca.regielive.ro/laboratoare/retele/protocolul-nat-retelele-netware-239957.html